STATE OF MICHIGAN

JOHN ENGLER, Governor

DEPARTMENT OF STATE POLICE

714 SOUTH HARRISON ROAD, EAST LANSING, MICHIGAN 48823

COL. MICHAEL D. ROBINSON, Director

January 12, 2000

TO: Senate and House Appropriation Subcommittees for State Police/Military and Veterans Affairs

RE: Enrolled Senate Bill No. 371 *Sec.* 1103 (1) *"If is the intent of the legislature that the department of state police explore the feasibility of establishing an Internet crime unit within criminal investigations. "*

As stated above, the Department of State Police has been directed by the Legislature to explore the feasibility of establishing an Internet crime unit within criminal investigations and report its findings to the appropriations subcommittees on State Police/Military and Veterans Affairs.

This report was prepared by the Investigative Services Bureau after an analysis of the scope of the problem and possible remedies to fight Internet and computer crime in Michigan,

The report contains conclusions reached by the researchers and suggestions for implementing an Internet and Computer Crime Investigative Unit within criminal investigations of the Michigan State Police, Investigative Services Bureau.

Should you have any questions regarding this report or the contents therein, please feel free to contact Insp. Robert Manes of the Field Detective Division at (5 17) 336-653 1.

Sincerely,

DIRECTOR

The Feasibility of Establishing an Internet Crime Unit In Michigan

Michigan State Police
Investigative Services Bureau
January 2000

Table of Contents

EXECUTIVE SUMMARY

National Perspective on Computer Use and Crimes

Projected Internet Population Growth in Millions

1996	1997	1998	1999	2000
37.84	58	87.75	110.25	132.75

- Estimated growth of the Internet is 40% per year.
- An estimated 14 million children use the Internet.
- 58 million people, age 3 and older, surfed the Internet in 1997.
- In 1998, Web connectivity in public schools increased to 89%.
- U.S. Department of Justice estimates cost of electronic crime as high as $10 billion per year.

Reporting of Computer Crimes

It is difficult to accurately quantify the extent of computer-related crime because it is not captured in the Federal Uniform Crime Report or the Uniform Crime Report (UCR) for the State of Michigan. Crimes that involve the use of computers are usually designated by the most serious charge in the UCR, i.e. sending a threatening e-mail to a subject would be categorized by the most serious offense; the threat.

Available data collected from January 1999 through September 30, 1999, indicates law enforcement personnel in Michigan have investigated over 300 Internet and computer-related crimes, including over 100 cases of Internet crimes against children as well as fraud, embezzlement, threats and hate crimes, money laundering, vandalism, terrorism and bomb threats, and homicide. *(See Appendix B.)*

Trends

As awareness increases, the number of crimes reported increases. As society becomes more familiar and dependant on technology, the opportunity for criminals to pursue traditional crimes on the information super highway also increases.

State Perspective on Computer Use and Crimes

- It is estimated that 6.5 million computers are used in Michigan.
- Most schools begin computer training at the elementary school level.
- Types of computer-related crimes being investigated in Michigan include homicide, counterfeiting/forgery, child pornography/criminal sexual conduct, fraud, threats, larceny/embezzlement, and hackers.

In 1998, the MSP Computer Crime Unit investigated 35 cases of computer crime. In the first six months of 1999, 52 cases were investigated. Of those, 80% were assists to other agencies. Five MSP personnel are self-taught in the area of computer crimes and working on computer-related investigations causes delays and backlogs in their workload. Due to the workload, some computer forensic examinations have been delayed by three months.

Proposed Internet Crime Unit

Annual costs to staff two investigative units, as proposed, would be approximately $1.288 million. Total recommended personnel for two teams, one in Lansing and one in Livonia, would include 12 FTE's; 7 detective troopers, 4 forensic information tech specialists, and 1 secretary.

MSP's Leadership Role

- To create and strategically locate Internet/Computer Crime units to improve the response time and quality of investigations of computer-related crimes.
- To provide and strategically place personnel who can assist investigators with computer forensics.
- To train police personnel and increase public awareness to prevent computer crime.
- To improve effectiveness and efficiency through cooperation with other agency investigators tasked with addressing computer crime.

FEASIBILITY STUDY

INTRODUCTION

The Department of Michigan State Police was directed by the 90th Legislature within Enrolled Senate Bill No. 371, an act to make appropriations for the department of state police, under the general heading, CRIMINAL INVESTIGATIONS, as follows:

Sec. 1103.(1) It is the intent of the legislature that the department of state police explore the feasibility of establishing an Internet crime unit within criminal investigations.

(2) The department shall report its findings to the appropriations subcommittees on state police/military and veterans affairs on or before January 15, 2000.

This report contains the findings and recommendations of the Michigan Department of State Police and supporting documentation regarding the feasibility of establishing an Internet crime unit within criminal investigations.

In May 1999, a multi-agency and multi-discipline Computer Crimes Project Team formulated recommendations for computer crimes investigative teams within the Michigan State Police. An executive summary of the final Computer Crimes Project Team Report dated May 13, 1999, has been documented in *Appendix A*, and this report is partially based on these recommendations.

The following areas have been addressed within this document in order to outline the feasibility and recommendations for an Internet Crime Unit.

- Internet and computer crime defined
- Scope of the Internet and computer crime problems to be addressed
- Overview of the national, state, and local data and cases
- State and local perspectives
- Recommended role of the Michigan State Police
- Recommendations and proposal summary, including budget considerations, personnel, equipment and training.

INTERNET AND COMPUTER CRIME DEFINED

Michigan Compiled Law 752.796(6) states, “A person shall not utilize a computer program, computer system, or computer network to commit a crime.” Computer crime can be divided into three categories: 1) the “computer as a tool” as in child exploitation, fraud, or embezzlement; 2) the use of the computer as “incidental” to other crimes as in

threatening letters; 3) and the "computer as a target" as in hacking. Additional descriptions of Internet and computer crime are listed in *Appendix B.*

The Legislature has recognized the increasing threat of computer crimes and recently passed two bills, Public Act 32 of 1999 and Public Act 33 of 1999. These prohibit a person to use a computer to commit, attempt to commit, conspire to commit, or solicit another person to commit a crime as well as prohibiting the dissemination of sexually explicit materials to minors via the Internet.

SCOPE OF THE PROBLEM TO BE ADDRESSED

OVERVIEW

It is difficult to accurately quantify the extent of computer-related crime as it is not captured separately in the Federal Uniform Crime Report (UCR) or the Michigan Uniform Crime Report. There is no specific category entitled "Internet or Computer-Related Crime," so law enforcement does not specifically track or categorize computer-related crimes. Crimes that involve the use of computers are categorized by the most serious charge in the UCR, i.e. the use of the Internet to electronically transfer child pornography would be categorized by the sexual offense. Data contained in this report is based on a study of the current problems.

NATIONAL PERSPECTIVE

Computer technology has exploded within the past decade providing easy access to large amounts of information and generating infinite opportunities for industry, trade, and private individuals to commit crimes. Information that was once difficult to obtain is readily available at the click of a mouse.

Access to the Internet is one reason for the tremendous increase in computer use in the last decade as one in five, or 57 million people, age 3 and older, surfed the Net in 1997. About 92 million adults, 47%, used a computer at work, home, or school. Half of all children in 1997 had a computer at home. Almost 14 million children use the Internet. Statistics indicate high usage of the Internet within rural, urban, and central cities. (National use of computers and the Internet is graphically portrayed in *Appendix C* to illustrate the demographic information regarding individuals accessing the Internet nationwide, by age and locale. Also included is a projection through the year 2000 of the ages of Internet users.)

As society becomes more familiar and dependent on technology, the opportunity for criminals to pursue traditional crimes on the information super highway also increases. While criminal activity involving computer technology has existed since the advent of the computer, the sheer number of computer crimes seems to have exploded with the introduction of the Internet. Within the last few years, the Internet has become the catalyst for other traditional crimes.

Nationally, the U.S. Department of Justice estimates dollar cost of electronic crime as high as $10 billion per year. A 1998 survey by the FBI and the Computer Security Institute of 520 computer security practitioners recorded financial losses from security breeches alone at $136.8 million, an increase of 36 % over loses estimated in 1997.

The Justice Department has in the past listed the most significant types of computer crimes as follows:

- Stealing tangible or intangible data
- Destroying or altering data
- Embezzling funds
- Destroying or altering software
- Producing/distributing child pornography

Many federal and state law enforcement agencies have initiated and funded Internet computer and high-technology crime investigative teams, including the FBI, Secret Service, Customs, and postal inspectors. Likewise, the states of Ohio, Illinois, New York, and Wisconsin in the Great Lakes region, and many other states including New Jersey, Massachusetts, Kansas, North Carolina, Oklahoma, South Dakota, Washington, Wyoming, and Florida have teams. Statistics show that the pool of potential offenders is constantly increasing and, to combat a subsequent amount of online deviance and crimes, high-technology investigative teams are being initiated to address the concerns and problems.

Appendix D outlines the history, activity, and personnel assigned to computer crime and high-technology investigative teams in Massachusetts, New Jersey, and New York.

In December 1999, a $300,000 grant from the United States Department of Justice was awarded to the Michigan State Police and Michigan Attorney General's office to help fight Internet Crimes Against Children, (ICAC). Nine other states also received similar funding. The grant will provide funds to enhance ICAC investigative efforts in Michigan. The three components of the grant include specialized ICAC training for state and local law enforcement officials, equipment purchases, and a public awareness and prevention campaign that will educate parents, children, and other individuals who use the Internet.

STATE AND LOCAL DATA AND CASES

Recent estimates place the number of computers in the state of Michigan at 6.5 million. The information technology industry has been identified as the state's fastest growing industry with 5,500 information technology companies and 3,000 software companies. Use of computers by adults and children continues to increase. The number of computers and computer training as well as use by students also continues to increase statewide. Many schools are requiring computer training at the elementary school level, and some schools have added computer labs to existing buildings. The rapid growth of computer technology for legitimate, and illegitimate use, continues to increase. The move toward

increasing computerization reflects Michigan's commitment to harnessing the information age; but it also poses potential problems due to the greater opportunities it provides for would-be-offenders. *Appendix E* provides Michigan population statistics by county along with school district enrollments. Also included are charts entitled "Kids and the Internet" and "Classrooms Online" which document the national perspective.

A questionnaire addressing computer crime was sent to all MSP posts and 39 randomly selected local departments. Results were documented by the Computer Crimes Project Team in December 1998. The following computer-related crimes were prevalent:

- Counterfeiting/Forgery
- Child Pornography/Criminal Sexual Conduct(CSC)
- Fraud
- Threats
- Larceny/Embezzlement
- Hackers
- Malicious Destruction of Property (MDOP)

The results of this survey also showed that most computer-related crime investigations required technical assistance to conduct the investigation. A large number of responses indicated that most investigations required some type of forensic assistance beyond the ability of the investigating officer.

Data was collected from January 1999 through September 30, 1999, that reports law enforcement personnel in Michigan have investigated over 300 Internet and computer-related crimes, including over 100 cases of Internet crimes against children. *Appendix F* documents the agencies providing this data and the number of computer-related crimes.

Appendix G provides examples of several Internet and computer crime cases investigated in all areas of the state including metropolitan Detroit, western Michigan, the northeast thumb area, northern Michigan, and the Upper Peninsula.

Appendix H documents known information regarding agencies and personnel available to address Internet and computer-related crime.

STATE AND LOCAL PERSPECTIVES

Internet and computer-related crime presents a challenge to Michigan's criminal justice system. Computer criminals are technologically sophisticated and generally one step ahead of the criminal justice system. Law enforcement's response to computer criminals has been seriously impeded due to lack of personnel, equipment, and training.

Based on contacts with local police departments statewide, law enforcement agencies are not prepared for officers to deal with Internet or computer crime complaints. Computer crime is technologically advanced and cannot be tackled through tactics learned at the

local police academy. Likewise, agencies do not have officers with the necessary training or equipment to deal with computer forensics.

- Law enforcement has not kept pace with the changes in the computer technology.
- Law enforcement officials lack expertise in the investigation of computer-related crimes and the retrieval of evidence.
- Most law enforcement agencies have little or no training or support in the investigation of computer-related crimes.

As Internet and computer-related criminal activity continues to rise at an alarming rate, the criminal justice system and law enforcement have not been provided personnel, training, and equipment necessary to keep up with this phenomena. As these types of cases arise, they are added to the caseload of a few self-taught investigators including uniform desk officers, post and narcotics detectives, and computer technicians, which causes delays in their workload. Also, the waiting period for assistance with computer forensic work is sometimes three months. Computer forensics is defined in *Appendix B.*

NEED:

Lack of a Coordinated Systematic Investigative Approach, Procedures, and Management of Computer-related Crimes

Michigan's law enforcement agencies are impeded in their efforts to successfully investigate, apprehend, and prosecute computer-related crimes due, in part, to:

- The absence of a systematic investigative approach and coordinated set of procedures for receiving, processing, and investigating complaints, as well as apprehension and prosecution of computer-related crimes;

- The lack of a network to support the needs of investigators in their efforts to manage computer-related crime case loads. If evidence isn't properly collected and preserved, a criminal case, or even the issuance of an arrest warrant, may be in jeopardy.

Preservation of the electronic crime scene requires risky decision-making. How should a suspect's computer be seized? Should a running computer be unplugged from the wall or systematically shut down based on the unit's requirements? Crippled by the absence of a systematic, coordinated investigative approach, procedures, and case management skills, Michigan's investigators lose critical time searching for answers. Where do I begin? How do I determine who created a Website? How do I determine who sent pornographic images via e-mail? I've never seen this technology before, what do I do now? Valuable information may have been erased or deleted, but can it still be retrieved? While these details may seem minor, they may have a significant impact on the results of an investigation. Investigators' fears are compounded by the fragility of computer evidence. Investigators typically lack the contacts, knowledge base, and physical resources to respond quickly to computer-related crime when it is reported.

Reported incidents of these crimes must be tracked as quickly as possible. This requirement stems from several factors: 1) system administrators often only maintain logs over a short time-frame averaging one to two weeks; 2) the intruder/perpetrator may currently be logged into the network and can be actively tracked only if a fast response is given by the investigator; 3) in the interim, other system users may have unknowingly and inadvertently altered the evidence.

Lack of Technological and Computer-Based Communications Skills and Knowledge of Laws, Regulations, and Procedures related to the Investigation, Handling of Evidence, and Prosecution

In comparison to the technological sophistication of some criminals, Michigan's law enforcement agencies are unprepared as evidenced by:

- The serious shortage of technologically proficient investigators trained in case management of computer-related crimes;

- The lack of state-of-the-art computer hardware and software programs essential to the investigation and apprehension processes;

- Lack of articulation of available human, programmatic, and technological resources to effectively manage computer-related crime investigations.

These types of crimes present a unique set of requirements to investigators. Cracking encryption schemes presents a challenge to computer crime investigators, even with the forensics software available. The unique nature of computer evidence means that it must be delicately handled from the moment it is seized. Likewise, protecting equipment to preserve authenticity is important. In court, prosecutors must prove that information taken from a computer was not modified or altered. Defense attorneys also have become savvy in computer crime issues, making it even more important to have the resources necessary to investigate this type of crime.

MICHIGAN STATE POLICE ROLE

The Michigan State Police must take a leadership role in developing and promoting a sound, long-range strategy for high-technology police work. This would include interagency and interjurisdictional cooperation and coordination, information networking, and technical training and equipment to address high-technology crime. The Michigan State Police is continually being asked to provide investigators to do these investigations and provide leadership and assistance with Internet and computer-related incidents. Local law enforcement also looks to the Michigan State Police to provide computer forensic expertise and assistance as well as training needs.

Since 1917, the Michigan State Police has been committed to providing direct support and assistance to local, county, and state public safety agencies. With the unique positioning of statewide resources and services, the Michigan State Police are committed

to providing highly trained personnel, high-technology equipment, and state-of-the-art technology to ensure that the public's safety remains the number one goal of all law enforcement agencies within Michigan's 83 counties.

ROLE

- To create and strategically locate Internet/computer crime units to improve the response time and quality of investigations of computer-related crimes.

- To provide and strategically place personnel who can assist investigators with computer forensics.

- To assist with training other departments and agencies.

- To improve and maintain communication with agencies who are experiencing computer crimes.

This role mirrors the Michigan State Police vision to ensure the safety of our citizens through the pursuit of innovations and initiatives, which coordinate and improve the collective efforts of the public safety and criminal justice systems. Our success in realizing this vision requires the agency to embrace change, aggressively employ new technology, and adopt progressive management, investigative, and enforcement practices.

The Michigan State Police recognizes its responsibility to provide support services not otherwise available to local components of the criminal justice community. The research and development of crime fighting technologies remain critically important in the ongoing effort to improve crime solvability. State level support and coordination must also be provided to public agencies at the local level to ensure an effective response to critical incidents. Just as specialized criminal investigative units and prevention programs for crimes of violence and drug use developed, similar investigative units need to be developed to address Internet and computer-related crime.

The Michigan State Police has been involved with investigating computer-related crimes since the early 1990's. The department has been involved in a broad spectrum of these types of investigations, including pornography, stalking, threats, destruction of property, hacking, gambling, and tax fraud as well as narcotics, homicide, and child exploitation cases.

In an attempt to address the Internet and computer crime phenomenon, the department currently has one officer assigned to a Computer Crime Unit in southeast Michigan assisting other departments in their computer crime investigations and computer forensic needs. In 1998, this unit investigated 35 cases of computer crime. In the first six months of 1999, 52 cases were investigated. Over 80% of the cases this investigator handles are being investigated by outside agencies.

While the Michigan State Police has a few officers who are "self taught" and who have investigated computer-related crimes, the department does not have a staff of adequately trained investigators who are dedicated full-time to these types of investigations.

OBJECTIVES:

- To establish and operationalize an adequate number of Internet and computer crime investigative units statewide to meet the needs of law enforcement.

- To enhance the technological and networking capabilities of this agency's existing resources to support local law enforcement agencies and departments.

- Enhance the ongoing efforts of the Michigan State Police and other local and federal law enforcement agencies to effectively respond to criminal cases involving the use of computers statewide.

- Improve the investigative techniques and abilities of Michigan's law enforcement and detectives currently being assigned investigations involving computers.

- Adequately train and equip the personnel to be assigned to the computer crime investigative units within criminal investigations. Additional training and equipment will allow these investigators and personnel to investigate computer-related crime as well as serve as a resource for all law enforcement agencies statewide.

- Lastly, systematically gather data regarding the severity of the computer crime problem in Michigan.

RECOMMENDATIONS

The Michigan State Police recommends the creation of two strategically located Internet and computer crime investigative units to address the problem of computer-related crime within Michigan's 83 counties. These units will significantly enhance the abilities of law enforcement agencies and departments statewide to combat those who utilize computers and other high technology equipment to commit crimes.

An Internet and Computer Crime Investigative Unit would be located in Lansing. This location, central within the state, would provide investigative services to all areas other than southeast Michigan. These investigators would maintain their own caseloads and provide technical assistance to agencies and departments within 73 counties in southern, central, western, and northern Michigan and the Upper Peninsula.

Due to the current volume of Internet and computer crime reported in southeast Michigan, it is recommended the investigative unit located at Southeastern Criminal Investigation Division in Livonia be expanded. These investigators would maintain their own caseloads and provide technical assistance to agencies and departments within 10 counties in southeast Michigan.

PROPOSAL SUMMARY

LOCATION/PERSONNEL

Total personnel recommended:

12 FTE's: 7 D/Tprs., 4 Forensic Information Tech Specialists (FITS), and 1 Secretary

Lansing:	4 D/Tprs.	Livonia:	3 D/Tprs.
	2 FITS		2 FITS
	1 Secretary		

COST ESTIMATES:

Yearly costs for personnel recommended to staff two investigative units as proposed would be approximately $1.28 million.

Personnel:	$951,348.
Computer/equipment costs:	105,950.
CSS&M:	77,201.
Fleet:	61,632.
Travel:	7,800.
Training:	84,000.
Combined total Both Units……	**$1,287,931**

APPENDIX A

EXECUTIVE SUMMARY
COMPUTER CRIMES PROJECT TEAM
FINAL REPORT and RECOMMENDATIONS
May 15, 1999

COMPUTER CRIMES PROJECT TEAM MEMBERS	
Insp. Robert Manes, Chair	MSP - Field Detective Division
F/Lt. Doug Ballard	MSP - Gladwin Post
Mr. Mark Blumer	Attorney General Criminal Division
Mr. Dan Dahlgren	MSP - Office of Special Projects
D/F/Lt. Mark Dougovito	MSP - CID, Lansing
Mr. Gary Ide	MSP-CJDC
Capt. Richard Lowthian	MSP - Forensic Science Division
D/F/Lt. David Minzey	MSP - Investigative Resources Section
D/Sgt. Robert Peplinski	MSP - SECID, Livonia
Lt. Steve Person	Lansing Police Department
Det. Steve Sergeant	Ingham County Sheriff Department
D/Sgt. Robin Sexton	MSP - St. Ignace
D/Lt. Glenroy Walker	MSP - Third District HQ, Saginaw

Several guests attended the meetings and provided valuable input including; Capt. Jack Shepherd, Michigan State Police (MSP) Executive Division; Judge Kirk Tabbey, Washtenaw County District Court; Messrs. William Richards, Robert Ianni, and Peter Plummer, Attorney General's Office; Messrs. Terry Berg and Patrick Corbett, U.S. Attorney's Office, Eastern District; Mr. Richard Murray, U.S. Attorney's Office, Western District; Agent Paul Kelly. U.S. Customs, Detroit; and Postal Inspectors Wallace Boyance and David Bosch, Detroit.

The committee was to review the scope of the problem, related training issues, the feasibility of a Forensic Computer Crime Center, what role the Michigan State Police should play in dealing with this expanding problem, and what resources will be necessary to adequately address the computer crime issue. The team was to report it's findings and make recommendations to the Michigan State Police Coordinating Council.

RECOMMENDATIONS:

A process should be implemented to capture statistical information regarding computer and high-tech related crimes statewide.

The Computer Crimes Project Team recommends a steering committee be developed from existing team members to act as a support mechanism for pending legislation, training needs, funding, and other issues that may arise related to the computer crime issue.

Basic computer crime investigation training should be offered to **all officers**.

APPENDIX A

Basic and advanced training and other specialized training on computer crime evidence recovery should be provided to **computer technicians.**

Computer forensic specialists should be required to have an advanced degree in Computer Science and advanced computer knowledge. Training of this individual would be on going as the technology changes and expands.

The Computer Crimes Project Team recommended that the MSP take a leadership role in developing and promoting a sound, long-range strategy for high-tech police work. This would include interagency and interjurisdictional cooperation and coordination, information networking, and technical training.

The Project Team recommended an 8 investigator unit be located in Lansing. This would allow the unit to be centrally located within the state. This will assist with access and response time and help lower the start-up costs, including the large amount of necessary laboratory equipment and other supplies. This unit would have a minimum of 7 detectives and 1 civilian computer forensic specialist. Due to the existing need for a unit in southeast Michigan, the team recommended 3 detectives be added to the existing unit at the Southeast Criminal Investigation Division. These officers would provide technical assistance to agencies and officers in southeast Michigan and maintain their own caseloads as time allows. Each location would also have a secretary assigned.

APPENDIX B – DEFINITIONS

❖ **Internet and Computer Crime** defined:

Most experts have agreed computer crime falls into 3 broad categories.

1) When a computer is a *tool of the crime*, the computer is used to commit a traditional crime utilizing high tech equipment and means. Many of these crimes are serious. Examples include:

- Utilization of computer equipment, including desktop publishing software, scanners, and digital cameras to forge fraudulent State of Michigan lottery tickets, license plate tabs, and cigarette stamps and other official documents.
- Embezzlement
- Distribution of child pornography
- Child exploitation
- Transfers of proprietary information
- Fraud, including Internet marketing scams
- Threats and Hate crimes
- Stalking
- Gambling and Money laundering

2) If a computer is the *target of a crime*, a criminal computer intruder attacks an innocent party's computer system. Some examples include:

- Trespass and Vandalism
- Sabotage
- Theft of intellectual property
- Threats of extortion
- Terrorist activities
- Unsuspecting individuals credit card numbers have been stolen and used to purchase items over the Internet

3) A computer is considered *incidental to a crime* if the computer is not required for the crime but is, in some way, connected to the criminal activity. Computers are often repositories for:

- Information and records of narcotics dealers
- Financial records of tax cheats
- A diary or itinerary of a homicide or rape suspect or victim
- Suicide notes and threatening letters
- Documentation saved by a suspected arsonist or terrorist or bomber.

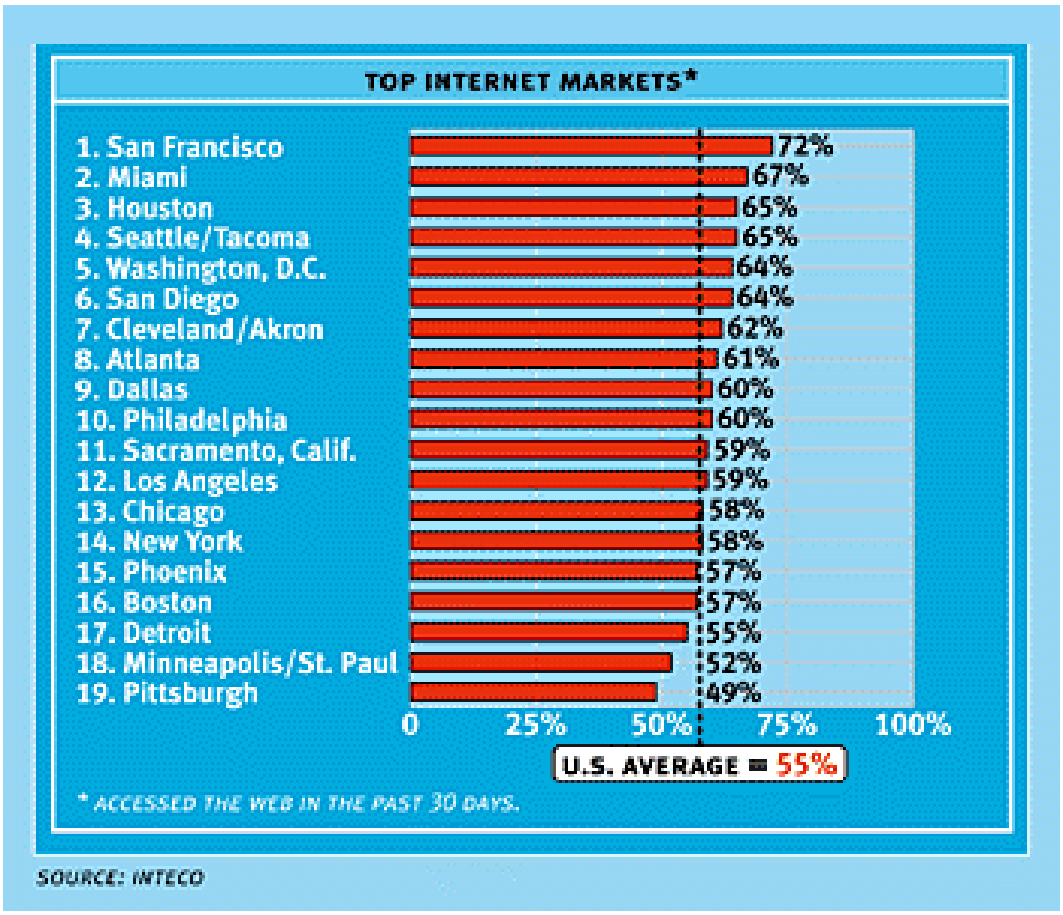
❖ **Computer Forensics** defined:

The discipline of obtaining evidence from a seized computer. This includes determining where the evidence is located within the computer, determining how it should be extracted and maintained in order to preserve the required chain of evidence, for admissibility and credibility, and presenting and explaining the methodology utilized during court proceedings.

1) Computer Forensic Data Analysis –

- Process in which computer evidence is analyzed
- Requires specialized training, tools and equipment
- Advance knowledge of computer hardware, networks and operating systems
- Admissibility depends on qualifications and actions of the analyst
- Chain of custody and integrity of evidence must be obtained

APPENDIX C


TOP INTERNET MARKETS*
1. San Francisco 72%
2. Miami 67%
3. Houston 65%
4. Seattle/Tacoma 65%
5. Washington, D.C. 64%
6. San Diego 64%
7. Cleveland/Akron 62%
8. Atlanta 61%
9. Dallas 60%
10. Philadelphia 60%
11. Sacramento, Calif. 59%
12. Los Angeles 59%
13. Chicago 58%
14. New York 58%
15. Phoenix 57%
16. Boston 57%
17. Detroit 55%
18. Minneapolis/St. Paul 52%
19. Pittsburgh 49%
0 25% 50% 75% 100%
U.S. AVERAGE = 55%
* ACCESSED THE WEB IN THE PAST 30 DAYS.
SOURCE: INTECO

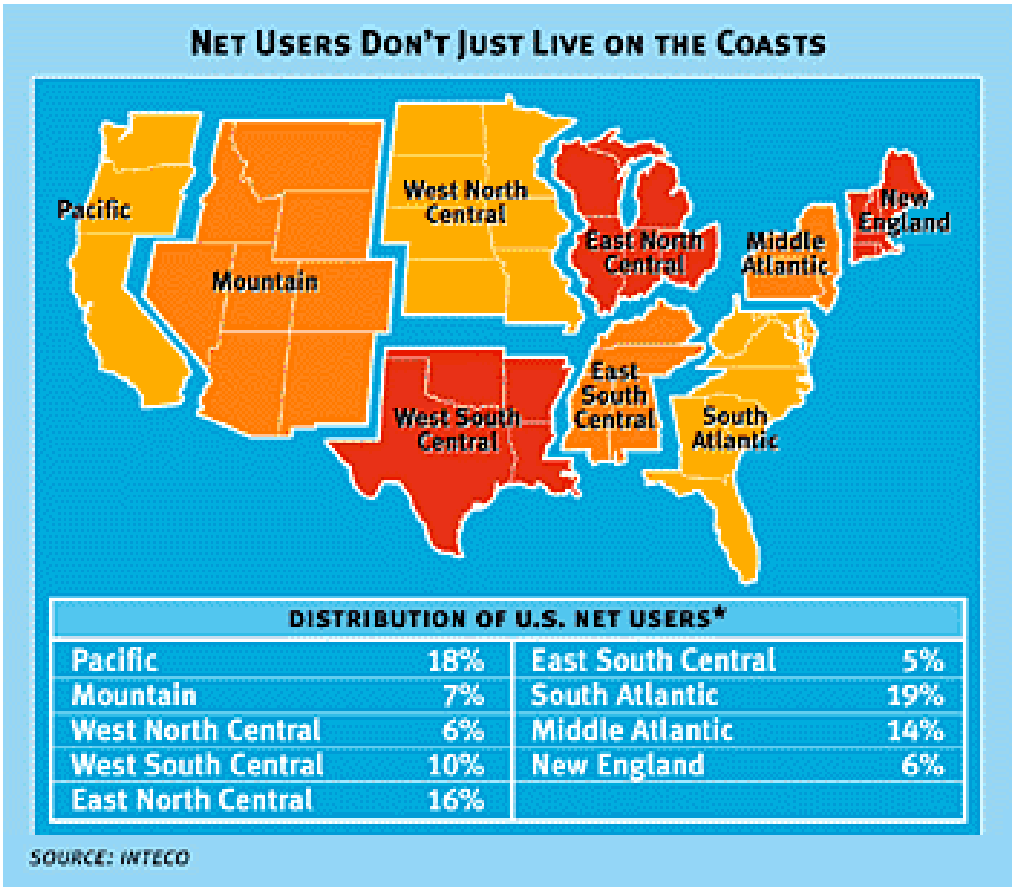
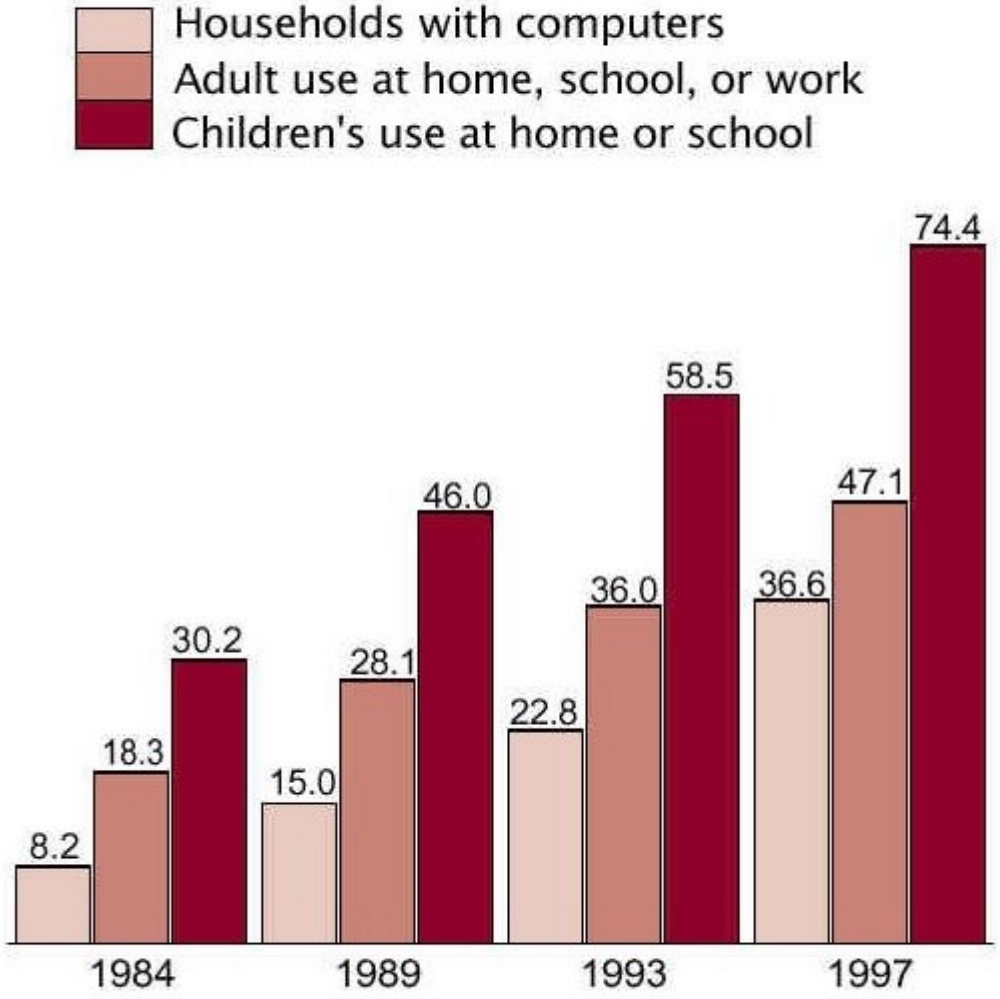

NET USERS DON'T JUST LIVE ON THE COASTS
Pacific
Mountain
West North Central
East North Central
Middle Atlantic
New England
West South Central
East South Central
South Atlantic
DISTRIBUTION OF U.S. NET USERS*
Pacific 18%
Mountain 7%
West North Central 6%
West South Central 10%
East North Central 16%
East South Central 5%
South Atlantic 19%
Middle Atlantic 14%
New England 6%
SOURCE: INTECO

Figure 1.

Computer Presence in the Home, and Use Anywhere, by Year

[In percent]



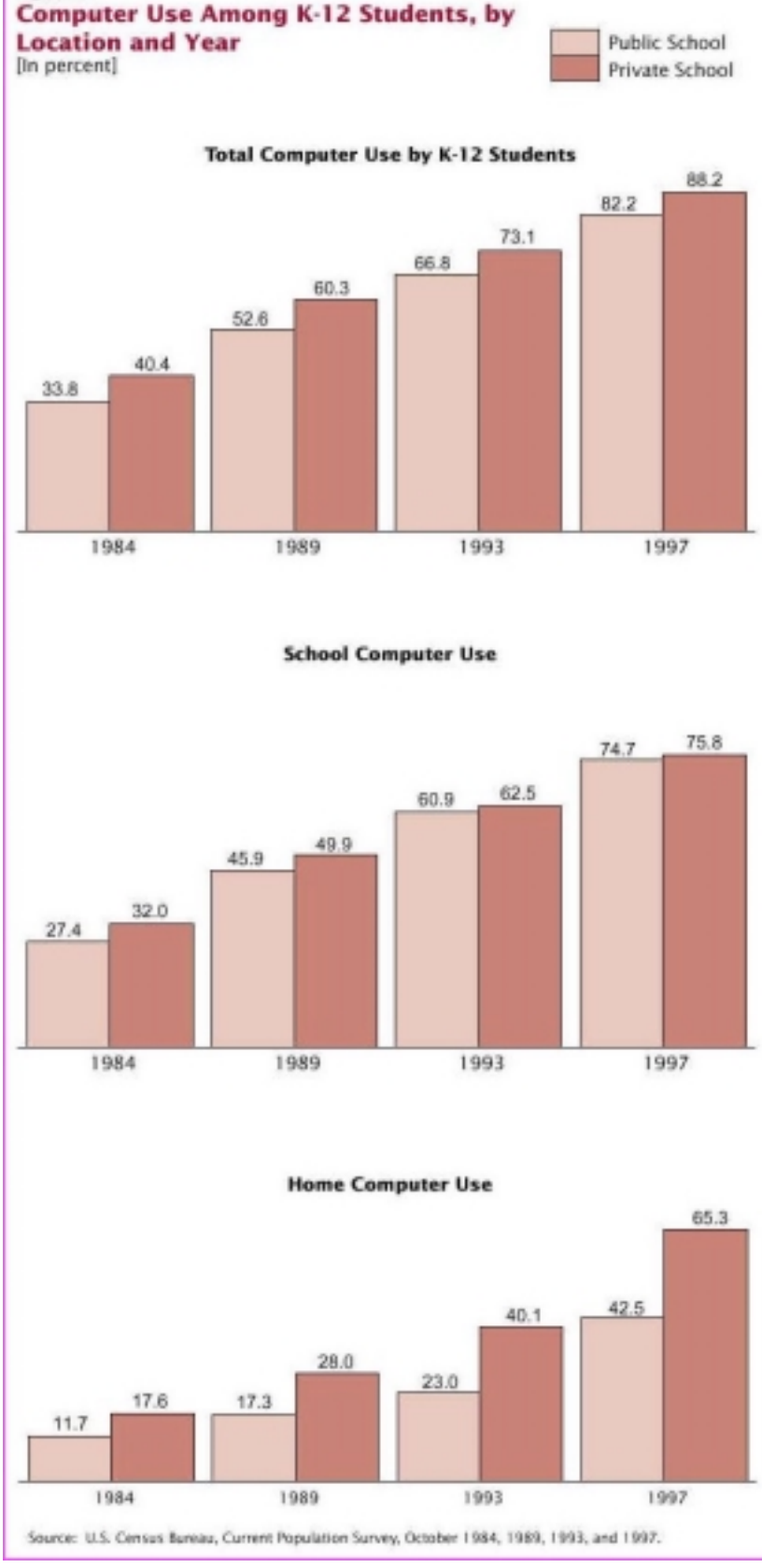
Source: U.S. Census Bureau, Current Population Survey, October 1984, 1989, 1993, and 1997.

APPENDIX C

Figure 2.

Computer Use Among K-12 Students, by Location and Year

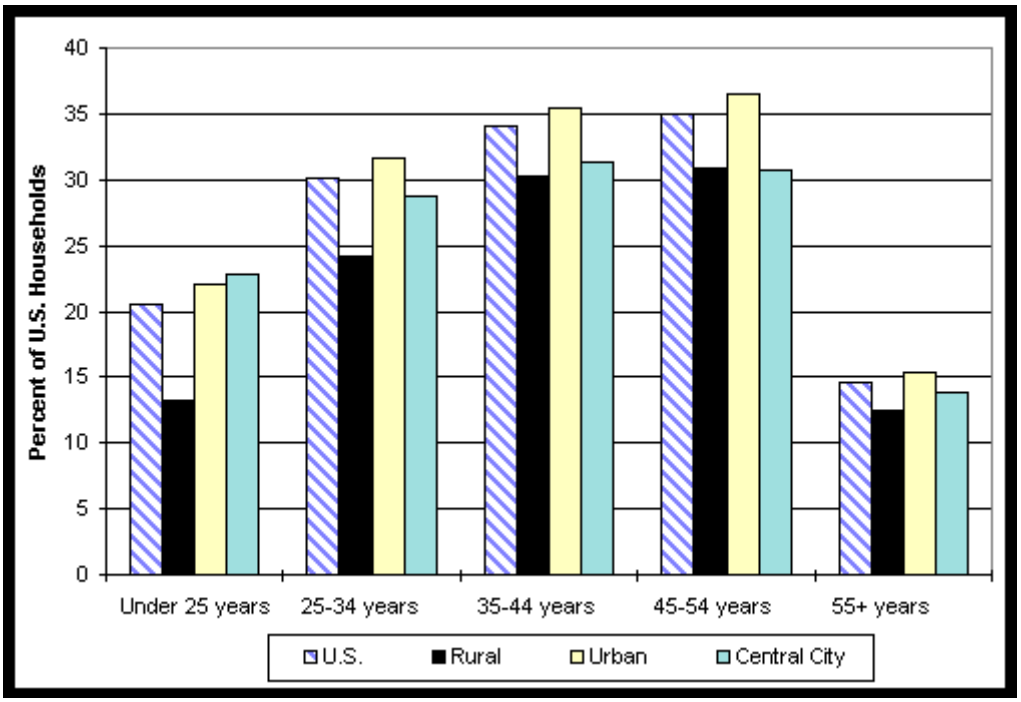
[In percent]



Source: U.S. Census Bureau, Current Population Survey, October 1984, 1989, 1993, and 1997.

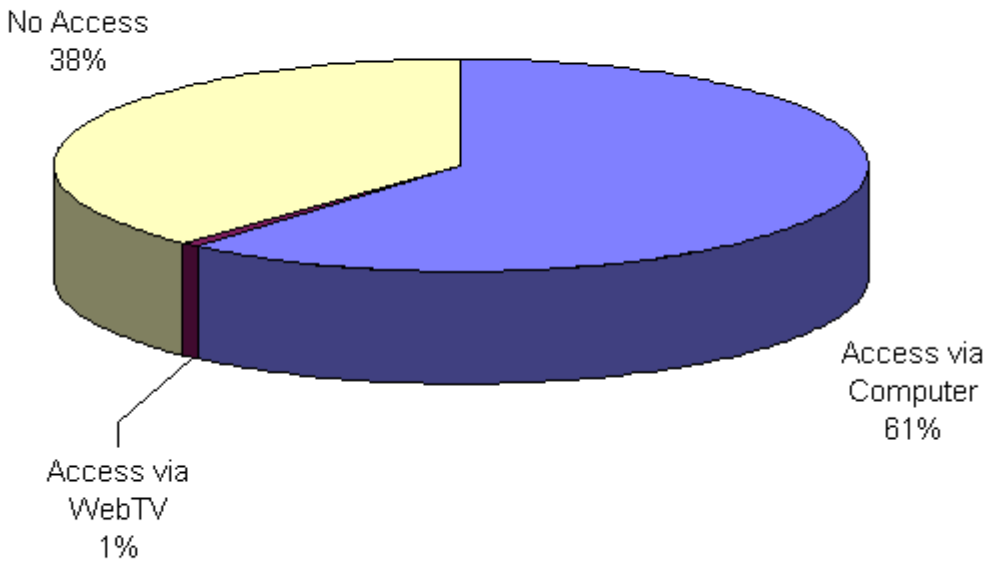
APPENDIX C

**Percent of U.S. Households Using the Internet By Age,
By U.S. Rural, Urban, and Central City Areas (1998)**



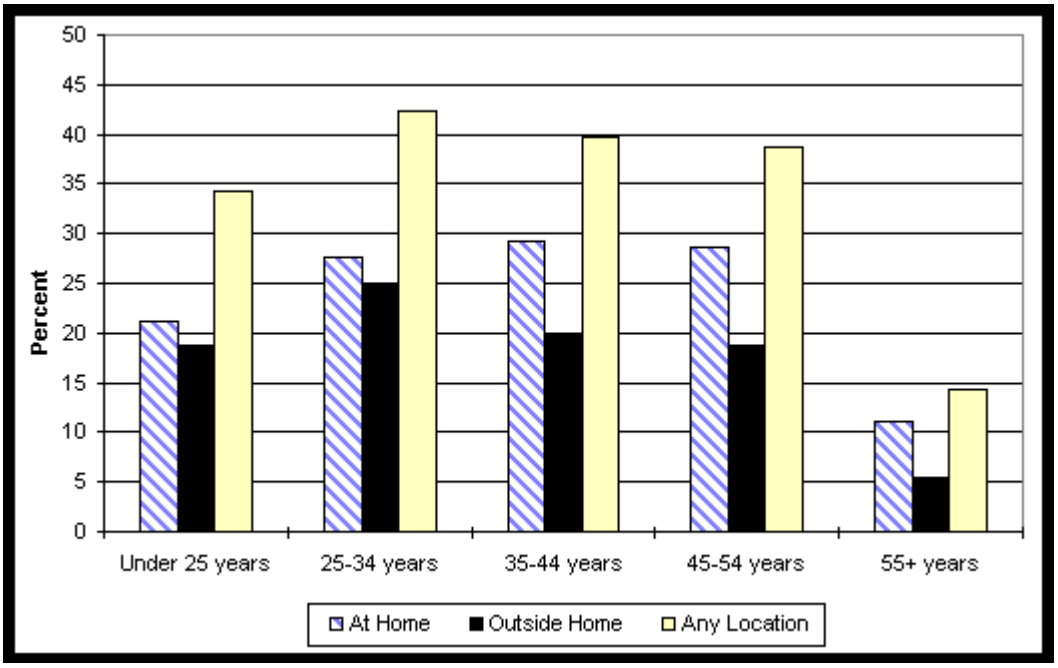
APPENDIX C

Percent of U.S. Households with a Computer/WebTV Accessing the Internet At Home

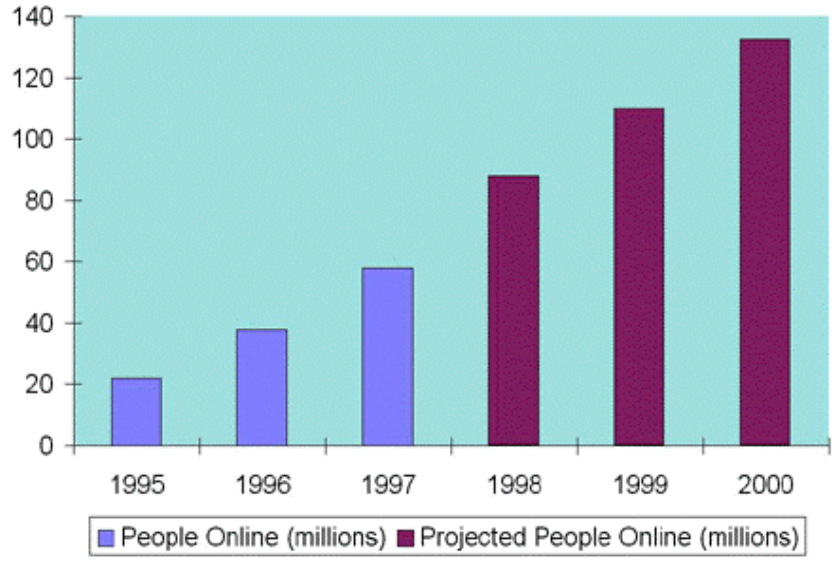


APPENDIX C

Percent of U.S. Persons Using the Internet By Age By Location (1998)



APPENDIX C



Internet Population Projected Growth

Date	Population (In millions)
1995	22
1996	37.84
1997	58
1998	87.75
1999	110.25
2000	132.75

Source: Fall 1997 CommerceNet/Nielsen Internet Demographic Survey (http://www.commerce.net/research/stats/wwwpop.html#IPOP)

APPENDIX D

Michigan State Police Feasibility Study

What Are Other States Doing to Combat Computer Crimes?

Massachusetts State Police

The Massachusetts State Police Computer Crimes Unit was formed in February of 1997. They handled 50 cases their first year and have investigated over 200 cases total so far through 12/1/99.

They started the unit with five people, one supervisor and four Troopers. They have maintained that number since 1997, and have posted openings for 2 additional Troopers, and 1 civilian computer technician.

The majority of the investigations are hackers, child porn, frauds, and narcotics related.

APPENDIX D

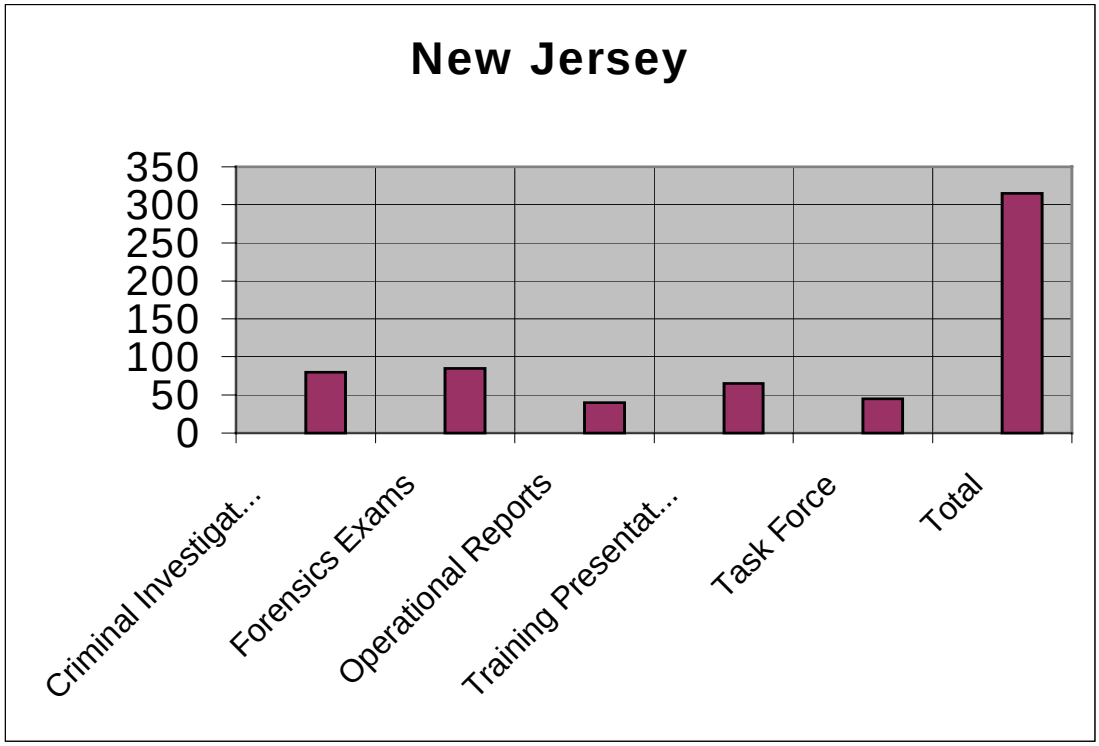
New Jersey State Police

The New Jersey State Police established a computer crimes unit in 1997 with 2 enlisted personnel.

As of December 1st, 1999, they have 10 personnel assigned to their Computer Crimes Unit.
1 Lieutenant
2 Sergeants
5 Detectives
1 Analyst
1 Clerical worker (They are requesting 2 civilian Forensic Examiners to be added by 1/2000)

They also have a Computer Crimes Task Force responsible for investigating Internet crimes against children. The Task Force consists of:
5 enlisted officers from various law enforcement agencies.
2 New Jersey State Police Officers
1 FBI Agent

APPENDIX D



Over 40% of all cases are child pornography. This includes both proactive and reactive cases.

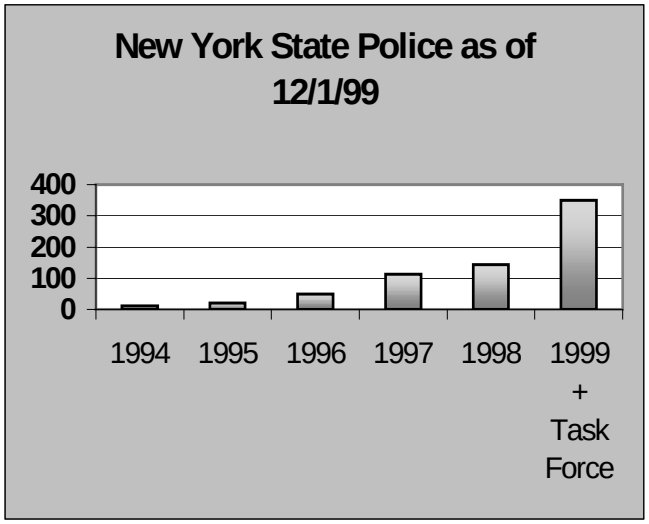
These units have worked homicides, corporate espionage, cases involving national security, narcotics, gambling, unauthorized access and destruction of data, and many other traditional crimes. This unit was responsible for the arrest of the subject who spread the Melissa Virus.

APPENDIX D

New York State Police

As a result of a university computer being "hacked" by someone who was not authorized to access it, the New York State Police formed a computer crimes unit in 1991. (NYSPCCU) At that time they assigned 2 Troopers. They now have 5 officers assigned, 4 in Albany and 1 in Marcie. The number of cases they investigate has risen dramatically over the last 5 years.

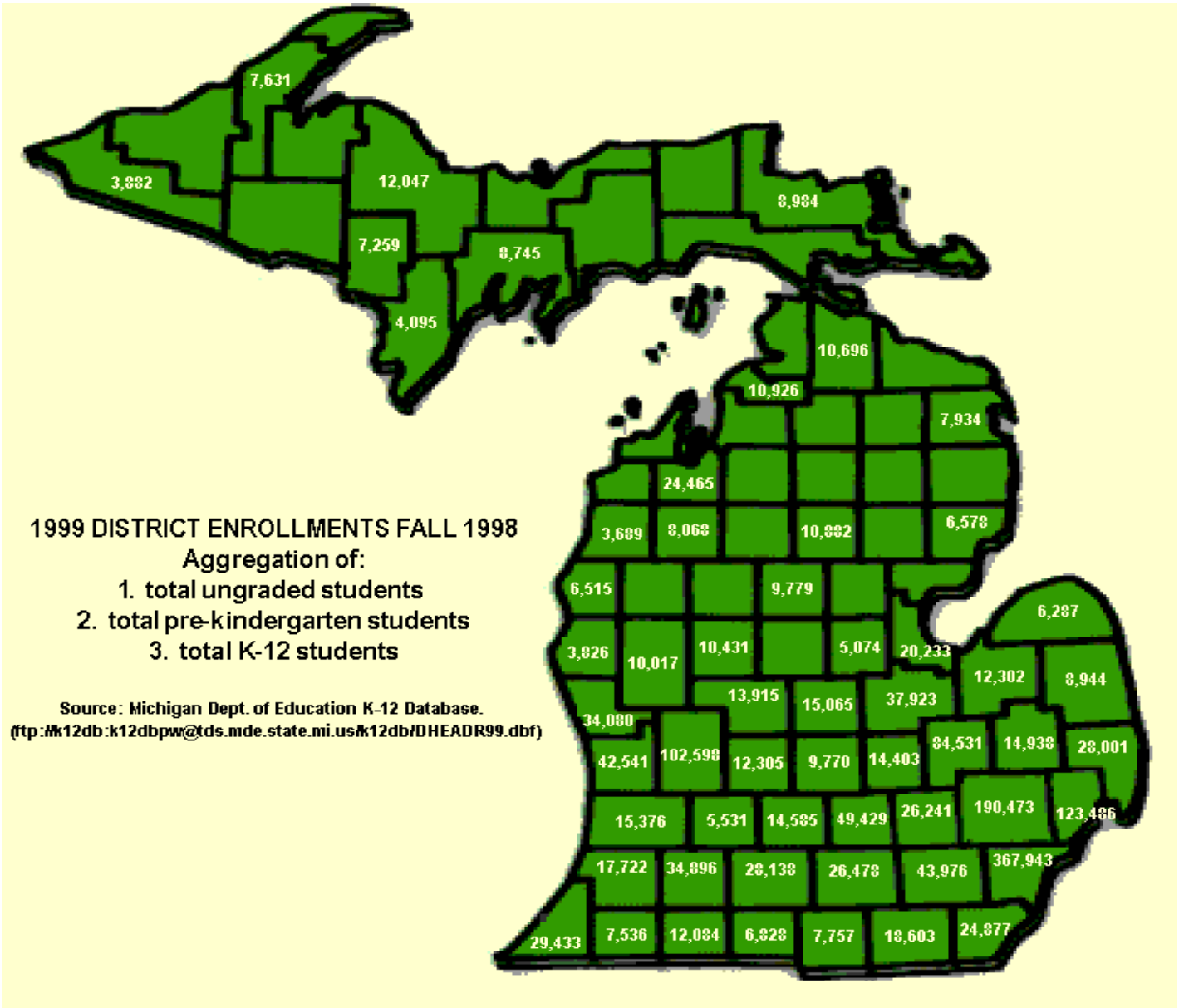
Number of cases last 5 years:
1994 - 12
1995 - 22
1996 - 50
1997 - 113
1998 - 144
1999 - 210+
(Add to this number the newly formed Internet Crimes Against Children Task Force, 2 officers – 140 cases through 12/1/99)



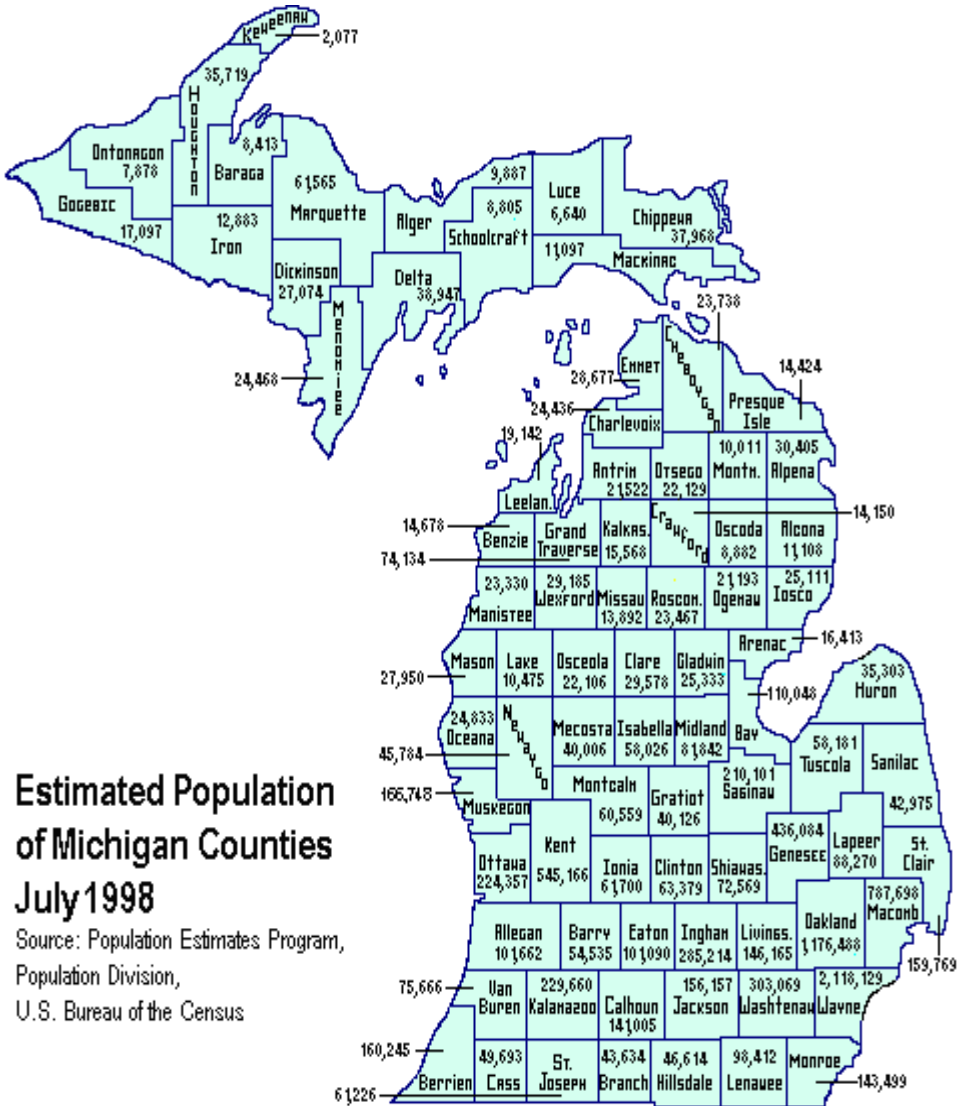
Eighty percent of this unit's work is forensics and obtaining evidence on traditional types of crimes where computers are being used to store the evidence, or commit the crime.

This next fiscal year, the New York Attorney General has requested 3 analysts' positions in their budget for computer forensics experts to assist the NYSPCCU in their computer crimes lab.

APPENDIX E


7,631
3,882
12,047
8,984
7,259
8,745
4,095
10,696
10,926
7,934
24,465
3,689
8,068
10,882
6,578
6,515
9,779
6,287
3,826
10,017
10,431
5,074
20,233
12,302
8,944
13,915
15,065
37,923
34,080
84,531
14,938
28,001
42,541
102,598
12,305
9,770
14,403
15,376
5,531
14,585
49,429
26,241
190,473
123,486
17,722
34,896
28,138
26,478
43,976
367,943
29,433
7,536
12,084
6,828
7,757
18,603
24,877
1999 DISTRICT ENROLLMENTS FALL 1998
Aggregation of:
1. total ungraded students
2. total pre-kindergarten students
3. total K-12 students
Source: Michigan Dept. of Education K-12 Database.
(ftp://k12db:k12dbpw@tds.mde.state.mi.us/k12db/DHEADR99.dbf)

APPENDIX E



Estimated Population of Michigan Counties July 1998

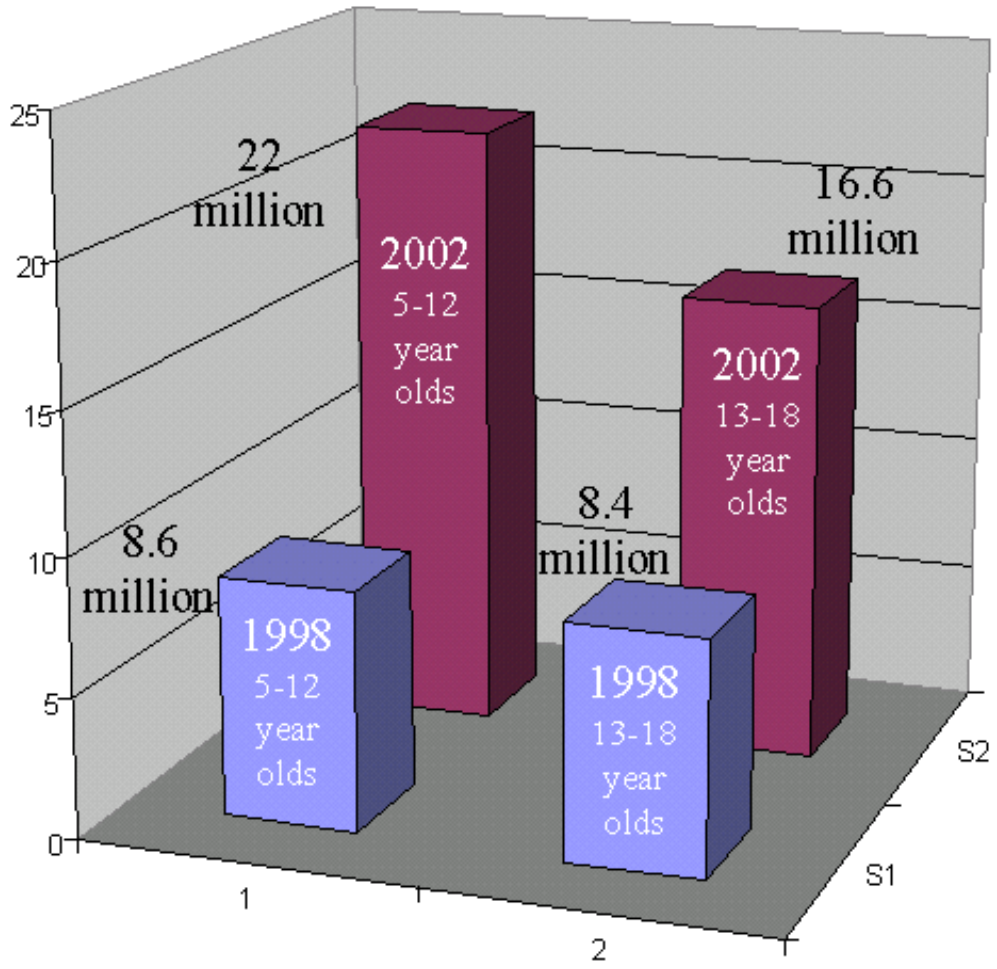
Source: Population Estimates Program,
Population Division,
U.S. Bureau of the Census

APPENDIX E

Kids and the Internet

KIDS ONLINE

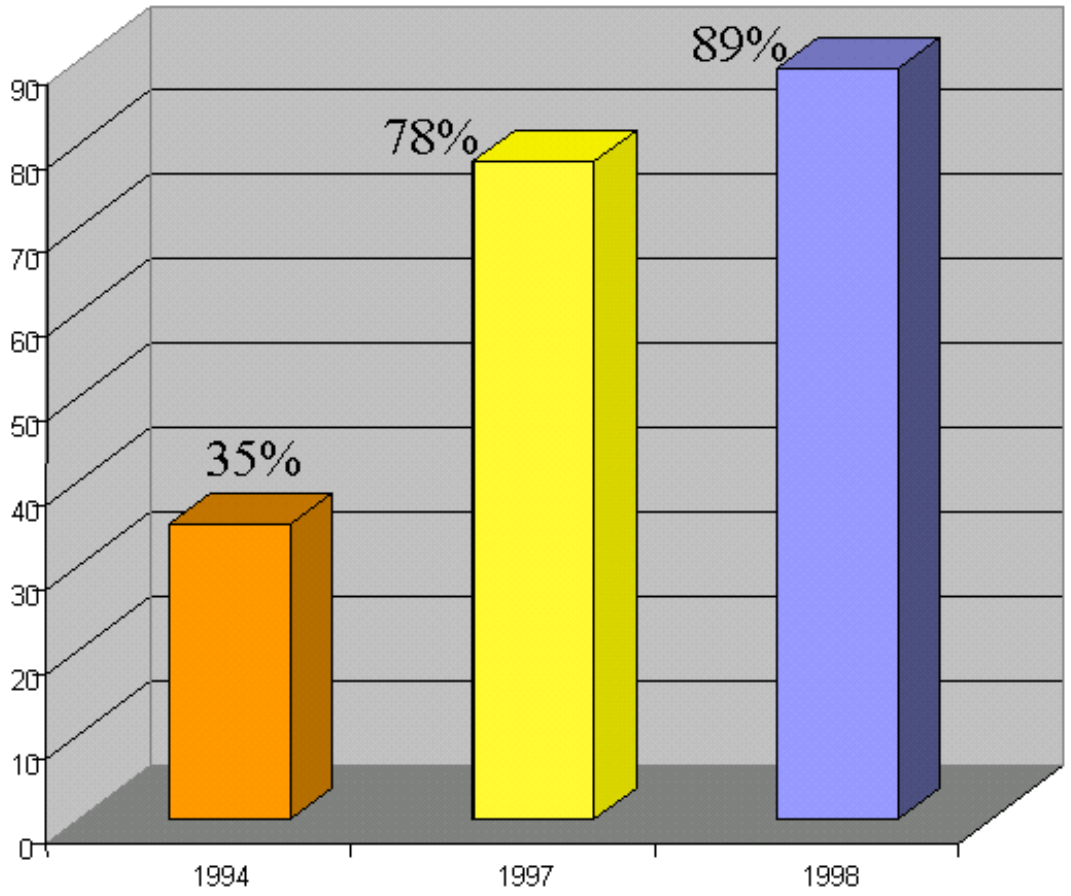
Last year, about 8.6 million kids ages 5 to 12 and 8.4 million ages 13 to 18 were online; Jupiter predicts the numbers will be 22 million and 16.6 million, respectively, by 2002.



APPENDIX E

Classrooms Online

From 1997 to 1998, Web connectivity in public schools increased to 89 percent.



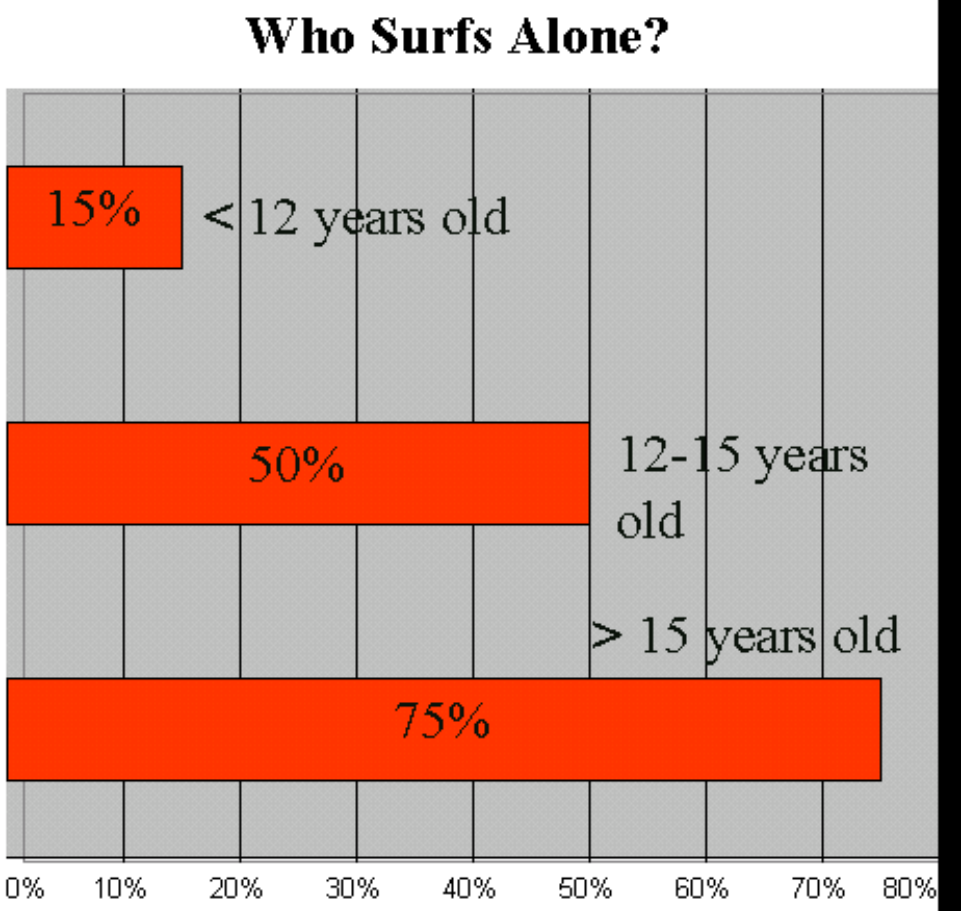
APPENDIX E

Kids and the Internet

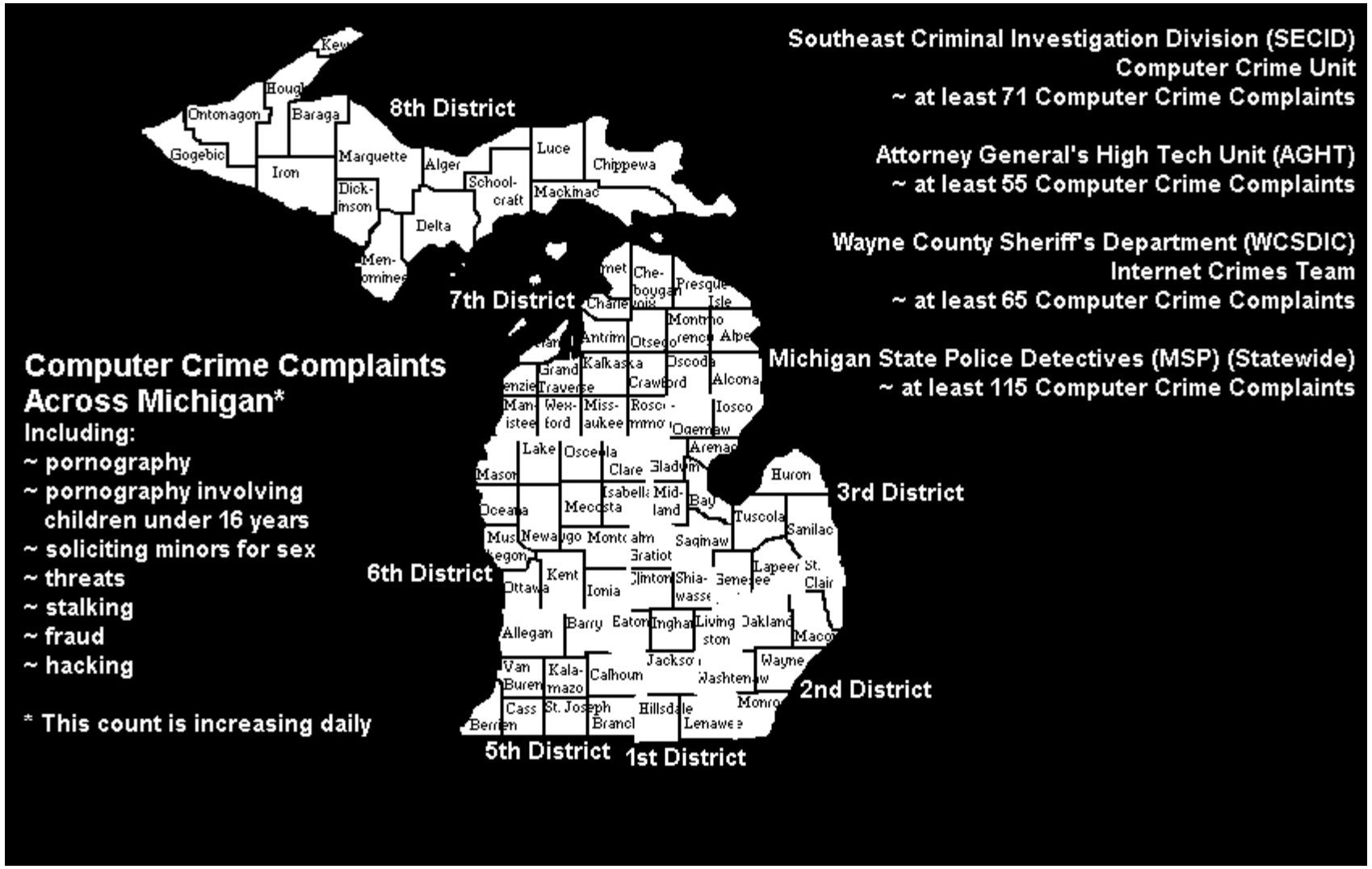
The majority of US children over the age of 12 are allowed to surf the Web unsupervised, according to a recent survey by Greenfield Online.

The study found that only 5 percent of parents with children over the age of 16 attempt to monitor their online activities, with just 20 percent of parents using software to control the type of material their children can access online.

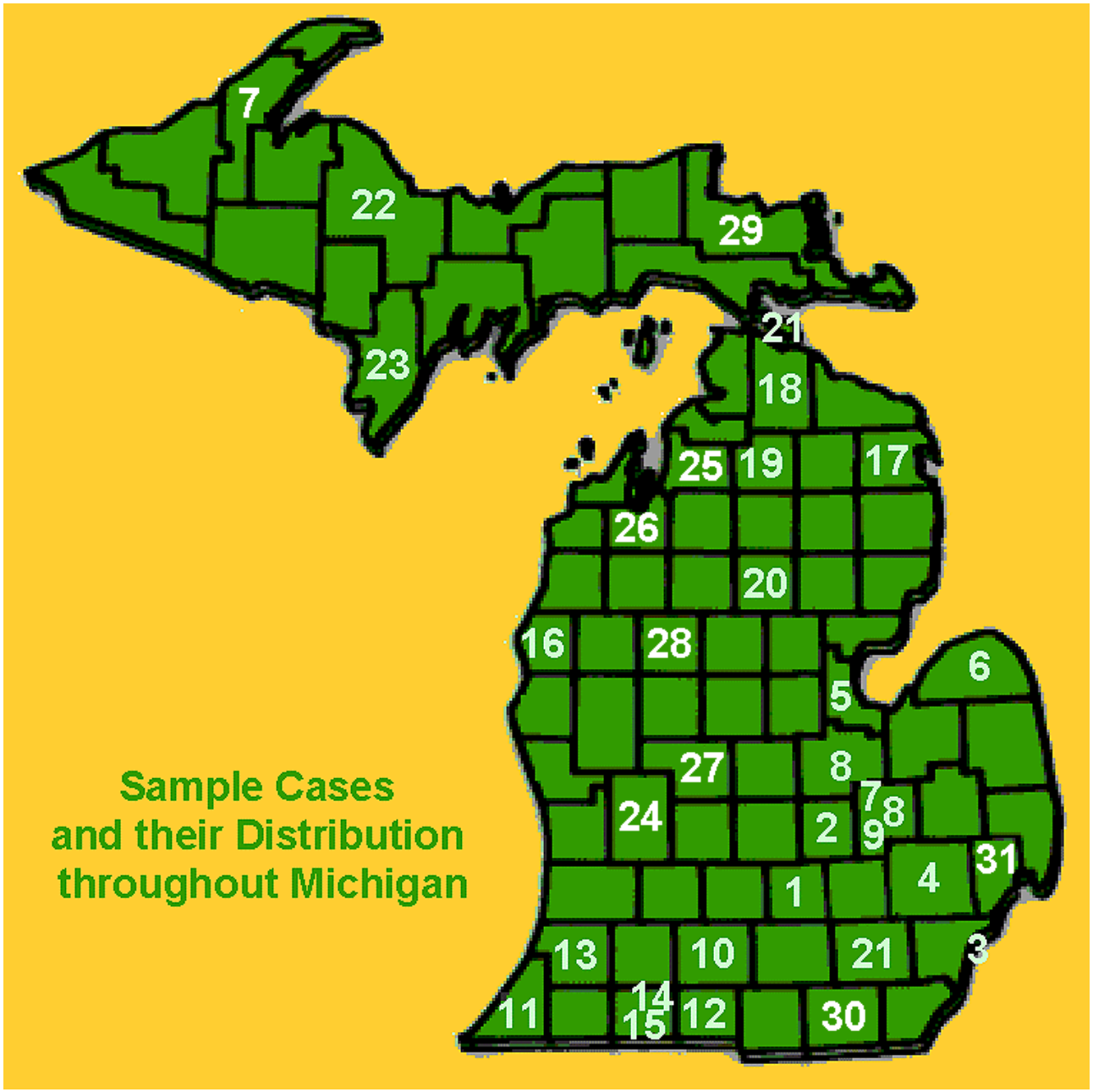
Greenfield estimates that 55 percent of children aged 11 and over use the Net for school work, while 20 percent of parents with children in this age group say that they are more interested in the Net than in TV.



APPENDIX F


Southeast Criminal Investigation Division (SECID)
Computer Crime Unit
~ at least 71 Computer Crime Complaints
Attorney General's High Tech Unit (AGHT)
~ at least 55 Computer Crime Complaints
Wayne County Sheriff's Department (WCSDIC)
Internet Crimes Team
~ at least 65 Computer Crime Complaints
Michigan State Police Detectives (MSP) (Statewide)
~ at least 115 Computer Crime Complaints
Computer Crime Complaints Across Michigan*
Including:
~ pornography
~ pornography involving children under 16 years
~ soliciting minors for sex
~ threats
~ stalking
~ fraud
~ hacking
* This count is increasing daily
8th District
7th District
6th District
5th District
1st District
2nd District
3rd District
Ontonagon
Baraga
Gogebic
Marquette
Iron
Dickinson
Alger
Schoolcraft
Luce
Chippewa
Mackinac
Delta
Menominee
Cheboygan
Presque Isle
Antrim
Otsego
Montmorency
Alpena
Kalkaska
Crawford
Oscoda
Alcona
Grand Traverse
Manistee
Wexford
Missaukee
Roscommon
Iosco
Ogemaw
Arenac
Lake
Osceola
Clare
Gladwin
Huron
Mason
Isabella
Midland
Bay
Oceana
Mecosta
Tuscola
Saginaw
Sanilac
Newaygo
Montcalm
Gratiot
Lapeer
St. Clair
Kent
Ottawa
Ionia
Clinton
Shiawassee
Genesee
Allegan
Barry
Eaton
Ingham
Livingston
Oakland
Macomb
Jackson
Wayne
Van Buren
Kalamazoo
Calhoun
Washtenaw
Cass
St. Joseph
Branch
Hillsdale
Lenawee
Monroe
Berrien

APPENDIX G


Sample Cases
and their Distribution
throughout Michigan
7
22
29
23
21
18
25
19
17
26
20
16
28
6
5
27
8
24
7
8
2
9
31
4
1
13
10
21
3
14
11
15
12
30

SAMPLE CASES-STATEWIDE

1. A subject recently hacked into the database of a **Lansing** area department. The subject discovered, and later disclosed, the names of informants involved in the Michigan State University riots.

2. Two **Shiawasee County** subjects met in a chat room. The male suspect obtained information from the female subject and began stalking her as a result.

3. Two males from **Windsor** arranged to meet a young teen age girl they met on the Internet at a **Howell** hotel. One of the subjects allegedly had sex with her.

4. A **Pontiac** male in his early twenties allegedly met a young teenage female in a chat room. He arranged a meeting with her and took her to his apartment and engaged in sexual intercourse. While investigating the complaint, the suspect's computer was seized and investigators located e-mail messages from the suspect to the victim from his computer.

5. In the **Bay City** area, a college instructor was embezzling funds through the use of a computer to falsify documents for illegal payments.

6. A bookkeeper at a **Caseville** business establishment was allegedly embezzling funds. The employee's computer was seized and searched for additional evidence.

7. In **Flint**, a local school teacher and a former student conspired to commit computer crime. They removed over 5000 files from the school's server. The former student knew the password and removed the files in **Genesee County** through the use of his personal computer at an **Upper Peninsula** university.

8. A **Frankenmuth** male in his twenties enticed a young teenage girl from **Clio** over the Internet. They met and allegedly had a sexual encounter.

9. A student hacked into the **Grand Blanc** High School computer system, causing a tremendous amount of havoc by changing grades and other school records.

10. In the **Battle Creek** area, a suspect was arrested for forging Michigan license plate tabs made on his home computer.

11. Threatening messages were sent via e-mail by a student in the **Bridgman** area promising to kill the underclassman if flex time was not going to be allowed at the school.

12. In the **Coldwater** area, police investigated a case where the suspect used an Internet chat room to proposition young girls for sex. He also sent nude photos of himself masturbating and of young subjects engaged in sex acts.

13. A subject in the **South Haven** area obtained credit cards in the names of other employees at a GM plant where he had computer access to their personnel files.

14. Three counterfeit $100 bills made with a computer scanner were passed at a store in **Sturgis**.

15. Data determined to be evidence of a double homicide in the **White Pigeon** area was retrieved from a lap top computer belonging to the suspect.

16. In **Ludington**, computer hackers were able to hack into a local web site design companies files causing havoc. The suspect's computer was seized for evidentiary purposes.

17. A computer was seized during a narcotics investigation in the **Alpena** area that provided important evidence of illegal activity. During this investigation, a methamphetamine lab was discovered and raided. The seized computer was searched and recipes for making methamphetamine and hash were found.

18. During the investigation of a **Cheboygan** home invasion, child pornography was discovered on the owner's home computer.

19. The computer of a subject in **Gaylord** was suspected to have had files deleted that may have been pertinent to an on-going criminal investigation. This made it necessary to have a computer forensic search of the computer.

20. A malicious destruction of property at **Kirkland Community College** in the **Roscommon** area was the result of a subject entering the college computer server by way of e-mail. Actions taken by the subject caused the entire system to crash.

21. **Mackinac Island** received several bomb threats this past summer. One particular threat was received via e-mail and tracked to a computer in the library of an **Ann Arbor** university.

22. A computer was seized and searched for records of narcotics activity during a significant narcotics investigation at the UPSET team in **Marquette**.

23. A suspect in the **Stephenson** area was reportedly having sexual relations with a young teenaged girl. The subject was sending love notes to the victim and the computer used to write these notes was seized.

24. A young boy in the **Grand Rapids** area was in a Pokemon chat room and was solicited for sex.

25. In **Antrim County**, a complainant found in a newsgroup the depiction of a young child performing fellatio on an adult subject.

26. Subjects in the **Traverse City** area obtained credit card information from a gas station credit card receipt and used it over the Internet to purchase memberships to pornographic sites.

27. A computer was seized from a physician during an investigation into a forged prescription case in the **Lakeview** area. Investigators were unable to search for possible evidence to the crime due to the complexity of the computer system.

28. A complaint was investigated where an older teen in the **Reed City** area was receiving threats via e-mails.

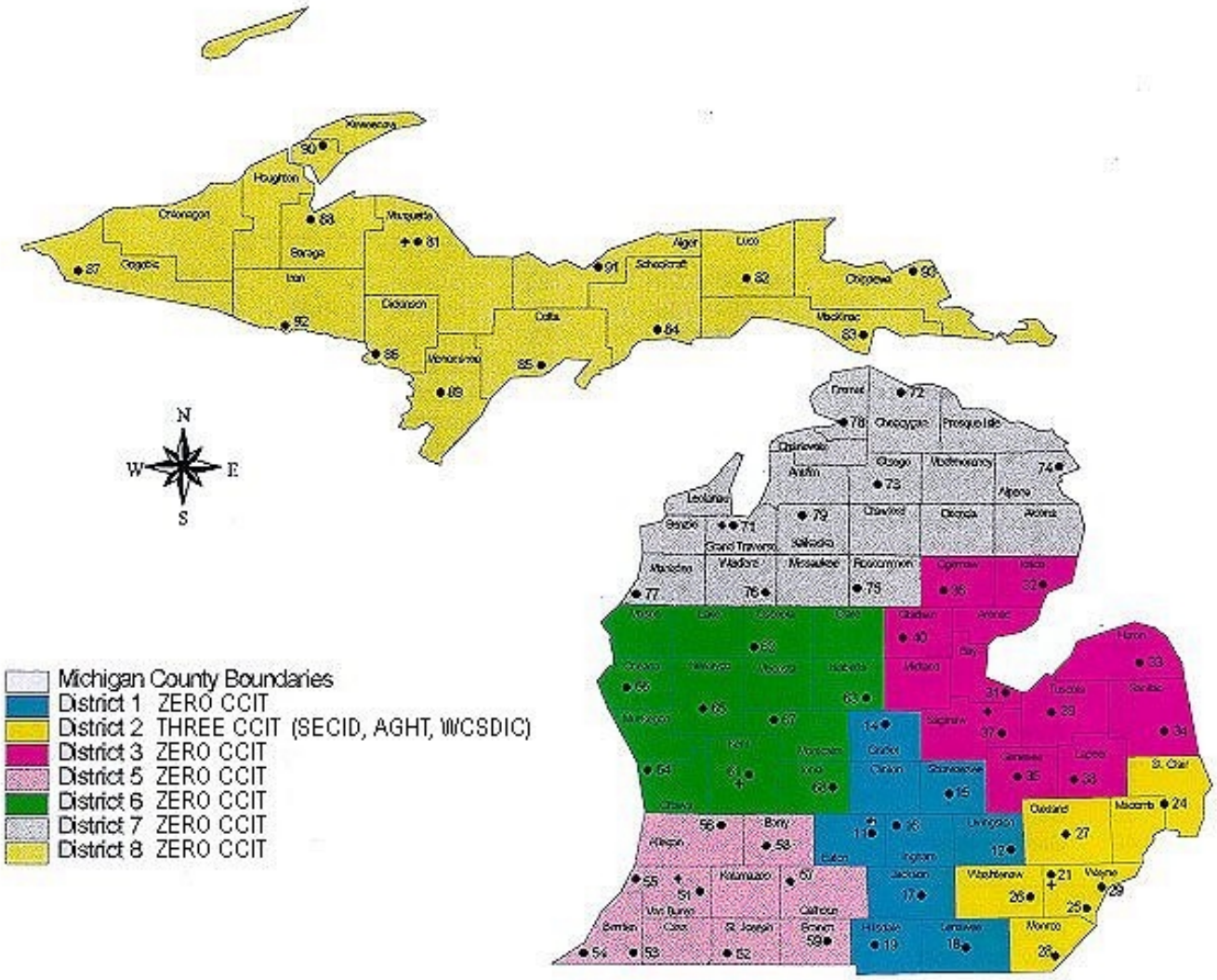
29. Threats were being sent by junior high students in the **Sault Ste. Marie** area to other students while attending school.

30. A female in her mid-twenties in the **Adrian** area was being stalked via computer at home and her place of employment.

31. An older male subject in **Macomb County** is being accused of posting child pornography and child erotica on the Internet.

APPENDIX H

COMPUTER CRIME INVESTIGATION TEAMS (CCIT) IN MICHIGAN BY DISTRICT, 1999



APPENDIX I

ACKNOWLEDGEMENTS

The following officials were invited to participate in this feasibility study. The research and preparation of this study was accomplished through the collaboration of many of these individuals.

Inspector Robert D.Manes
Michigan State Police
Field Detective Division
East Lansing, Michigan

Ms. Chris Wroblewski
Michigan State Police
Investigative Services Burea
East Lansing, Michigan

D/Sgt. Larry Dalman
Michigan State Police
Capitol Post
Lansing, Michigan

Ms. Nancy Becker
Michigan State Police
Budget Division
East Lansing, Michigan

Mr. Rob Olney
Michigan State Police
Budget Division
East Lansing, Michigan

Computer Crimes Project Team
Michigan State Police
Lansing City Police Department
Ingham County Sheriff's Department
Michigan Attorney General's Office
Lansing, Michigan

Matt Baker
Michigan State University
Research Assistant
East Lansing, Michigan

Win-son Chia
Michigan State University
Research Assistant
East Lansing, Michigan

Rebecca Grant
Michigan State University
Research Assistant
East Lansing, Michigan

Sameer Hinduja
Michigan State University
Research Assistant/Masters candidate
East Lansing, Michigan

Mr. Patrick Corbett
Michigan Attorney General's Office
High Tech Crime Unit
Detroit, Michigan